REMARKS

Claims 1-25 are pending in the Application. Claims 25-100 are canceled. Claims 1-25 have been rejected. Claim 1 is now amended.

Claims Rejections – 35 USC 112

The Examiner rejected claim 1 under 35 USC 112, first paragraph, as failing to comply with the written description requirement. More specifically, the Examiner asserted that the issue of the phrase "digital transfer via a computer communication medium..." has no support in the specification.

Applicant maintains that claim 1 as currently amended is fully supported by the specification.

Favorable reconsideration of this rejection is respectfully requested.

Claim Rejections – 35 USC 103

The Examiner rejected claims 1-25, under U.S.C. 103(a) as being unpatentable over US Patent Application No. 2005/0027617, to Jeffery Zucker et al in view of US Patent No. 7,069,249 to Stolfo et al.

As described in the summary of invention, the present application seeks to provide a novel method to facilitate fully anonymous purchases. Specifically, the current application provides methods that allow anonymous distribution and delivery of digital and/or physical entities, thereby allowing the buyer to remain anonymous throughout the entire buying process.

Zucker (U.S. Patent Application No. 2005/0027617), as described in the Abstract section, describes a method wherein a person registers at a privacy server and is given a pseudo identity that can be used to browse, register, purchase, pay for, and take delivery of products and services. Transactions are completed with the privacy server on a need-to-know basis. A seller communicates with the privacy server but only sees a demand, not the identity of the buyer. The financial institution communicates with the privacy server and sees the payment, not the merchandise. The freight company communicates with the privacy server and sees the package, not its contents. Although Zucker's privacy server operates in a manner that assures privacy and anonymity for the buyer and, if necessary, both the seller as well, all entities involved in the transaction are known to the privacy server. Further, the privacy server also has all data pertaining to the package.

Stolfo (US Patent No. 7,069,249), as described in the background of invention section, relates to transactions over a communications network between first and second parties, including ordering of a good and/or delivery of the good and/or payment for the good while securing private and personal information specific to the first party or the network device used by the first party with respect to the second party and unauthorized parties. However, with Stolfo a single party mediating between the buyer and seller may hold together information pertaining to buyer's identitiy, the seller's identity and the goods purchased by the buyer from the seller.

Claim 1 as currently amended, defines a computer-implemented method for making an anonymous computerized commerce transaction involving the delivery of digital merchandise comprising: sending first sensitive information from a computer associated with a first entity to a computer associated with a first intermediate entity; processing the first sensitive information at the first intermediate entity computer;

creating first non-sensitive information operable to approve the transaction by the first intermediate entity computer; sending the first non-sensitive information to a computer associated with a third entity operable to perform the transaction; performing the transaction at the third entity computer; and digitally transferring the digital merchandise to the first entity computer via a computer associated with a mediating delivering entity comprising information operable to deliver the digital merchandise to the first entity without revealing the first sensitive information to the third entity, wherein the *first intermediate entity computer is separate from the computer associated with the delivering entity.*

Preferred embodiments of the present invention teach the novel and inventive idea of a computer-implemented method for making an anonymous computerized commerce transaction involving the delivery of digital merchandise, wherein the *first intermediate entity computer is separate from the computer associated with the mediating delivering entity.*

That is to say, with the present invention sensitive information pertaining to the buyer of digital merchandise (say, the buyer IP address or credit data) may be hidden from the seller of the digital merchandise using a first intermediate entity's computer, the digital merchandise may be supplied to the buyer using a mediating delivering entity's computer, mediating between the seller and the buyer, for providing the electronic merchandise to the buyer without exposing details pertaining to the buyer (say, the buyer IP address) to the seller.

Using the novel and inventive idea of separating the first mediating party used for mediating the transaction with respect to financial aspects, and the mediating delivering entity used for mediating the transaction with respect to the supply of the digital merchandise to the buyer, there is achieved an improved level of data security

as no single party to the transaction, but the buyer himself, is exposed to both the buyer's identity data and the digital merchandise he buys.

A simplified exemplary embodiment is illustrated by the present application using Fig. 1 where an anonymous delivery service (150) mediates the delivery and thus holds data pertaining to the delivered item, whereas an acquirer (140) separated from the anonymous delivery service (150) mediates the payment made by the buyer of the item and thus holds financial data pertaining to the transaction, such as the client's credit card data. The vendor (130) is neither exposed to the identity of the client, nor exposed to the client's payment instruction details (say, the client's bank account number or credit card number) known only to the acquirer (140), nor exposed to the delivery information of the client (say, the client's e-mail box) known only to the anonymous delivery service (150).

Through separating the client's financial data and the client's delivery information, there is introduced an improved level of data security. For example, when the anonymous delivery service (150) is infected with a spyware such as a Trojan Horse, the spyware may be used to steal the client's delivery information, but the client's financial information remains safe with the acquirer (140).

Zucker as illustrated in Fig. 1 has a single privacy server (100) exposed to both delivery information of the client and financial information of the client, as well any additional information pertaining to the transaction.

Similarly, as illustrated by Stolfo's Fig.3E, Stolfo also uses a single entity, namely the proxy party, which holds all details pertaining to the first party (i.e. the buyer), including the buyer's credit approval data, the buyer's delivery address, etc.

Neither Zucker nor Stolfo describe or event hint at the novel and inventive idea of a method where *a first intermediate entity computer is separate from the computer*

associated with the mediating delivering entity, as taught by the present invention and defined by claim 1.

It is thus respectfully maintained that claim 1 as currently amended is allowable.

The remaining claims mentioned in this section of the Office Action are believed to be allowable as being dependent on an allowable main claim.

All of the matters raised by the Examiner have been dealt with and are believed to have been overcome.

In view of the foregoing, it is respectfully submitted that all the claims now pending in the application are allowable.

An early Notice of Allowance is therefore respectfully requested.

Respectfully submitted,

Martin D. Moynihan
Registration No. 40,338

Date: July 5, 2007

Encl.:
Petition for extension of time (1 month)